(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110336657 B
(45)授权公告日 2022.02.08

(21)申请号 201910592164.0
(22)申请日 2019.07.03
(65)同一申请的已公布的文献号
申请公布号 CN 110336657 A
(43)申请公布日 2019.10.15
(73)专利权人 上海大学
地址 200444 上海市宝山区上大路99号
(72)发明人 吴雅婷 李春华 张倩武 李正璇 孙彦赞 王涛
(74)专利代理机构 上海上大专利事务所(普通合伙) 31205
代理人 陆聪明
(51)Int.Cl.
H04L 9/00(2006.01)
H04L 9/08(2006.01)
H04B 10/70(2013.01)

(56)对比文件
CN 108718234 A,2018.10.30
CN 103167490 A,2013.06.19
CN 108768443 A,2018.11.06
CN 106102049 A,2016.11.09
CN 105721151 A,2016.06.29
CN 109600222 A,2019.04.09
CN 106059758 A,2016.10.26
CN 108366370 A,2018.08.03
EP 1463255 A1,2004.09.29
CN 103402200 A,2013.11.20
CN 106209355 A,2016.12.07
Yahya Mohammed Al-Moliki.Secret Key Generation Protocol for Optical OFDM Systems in Indoor VLC Networks.《IEEE Photonics Journal》.2017,

审查员 朱华慧

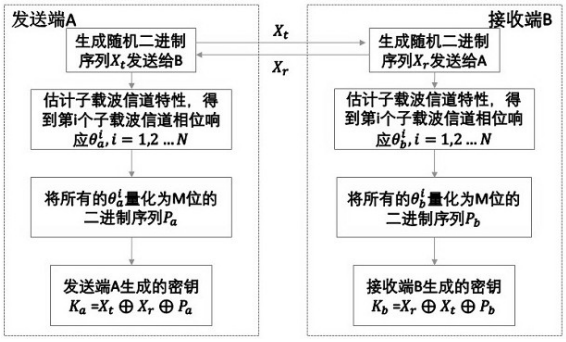
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种基于信道特性的光OFDM动态密钥生成方法

(57)摘要

本发明公开了基于信道特性的光OFDM动态密钥生成方法。本方法实现的步骤为:(1)通信双方分别生成一段随机探测信号,同时发送给对方;(2)通信双方接收到步骤一中的探测信号后各自估计信道特性;(3)通信双方各自取步骤二中所得到的各个子载波信道特性的相位值进行量化并生成一段二进制序列;(4)通信双方将上述本地生成的随机探测信号与对方发送过来的随机探测信号以及步骤三各自量化后的相位二进制序列依次进行异或得到最终所需的动态密钥。该方法有效利用了通信双方的信道特性以及本地私有的随机二进制信号动态地改变密钥,并有效地提高密钥的随机性,所获得密钥可以进行物理层加密相关操作,适用性强,保密能力突出。



CN 110336657 B

1.一种基于信道特性的光OFDM动态密钥生成方法，其中所生成的密钥是本地随机信号、发送端信号与量化后的信道相位的异或结果，其特征在于，包括步骤如下：

步骤一、发送端A生成随机二进制序列X_t并发送给接收端B；相干时间内，接收端B生成随机二进制序列X_r发送给发送端A；

步骤二、发送端A估计携带信号X_r的N个子载波的信道特性，得到通信双方的信道响应：$|H_a^1|e^{j\theta_a^1}$，$|H_a^2|e^{j\theta_a^2}$，…，$|H_a^i|e^{j\theta_a^i}$，…，$|H_a^N|e^{j\theta_a^N}$，其中N表示子载波总数，j表示虚数单位，θ_a^i表示发送端A的第i个子载波的信道相位，$|H_a^i|e^{j\theta_a^i}$表示发送端A第i个子载波的信道响应；接收端B估计携带信号X_t的N个子载波的信道特性，得到通信双方的信道响应：$|H_b^1|e^{j\theta_b^1}$，$|H_b^2|e^{j\theta_b^2}$，…，$|H_b^i|e^{j\theta_b^i}$，…，$|H_b^N|e^{j\theta_b^N}$，其中N表示子载波总数，j表示虚数单位，θ_b^i表示接收端B的第i个子载波的信道相位，$|H_b^i|e^{j\theta_b^i}$表示接收端B第i个子载波的信道响应；

步骤三、将发送端A所有的θ_a^i进行量化得到二进制相位序列P_a；同理，接收端B将所有的θ_b^i量化后得到二进制相位序列P_b；

步骤四、发送端A将得到的相位量化序列P_a与随机二进制序列X_r以及本地生成的二进制序列X_t进行异或运算生成密钥K_a；同理，接收端B将得到的相位量化序列P_b与随机二进制序列X_t以及本地生成的二进制序列X_r进行异或运算生成密钥K_b。

2.根据权利要求1所述的基于信道特性的光OFDM动态密钥生成方法，其特征在于：所述步骤一中随机二进制序列以一定的调制方式加载到一个OFDM的数据子载波上作为随机探测信号，其中随机序列长度同密钥位数一致。

3.根据权利要求1所述的基于信道特性的光OFDM动态密钥生成方法，其特征在于：所述步骤三中是将相位区间(0,2π]均分成Q个子区间，θ_a^i或θ_b^i落到相应的子区间内并进行对应的二进制编码，将发送端A所有的θ_a^i编码完成后按顺序合并为一个二进制相位序列P_a；将接收端B所有的θ_b^i编码完成后按顺序合并为一个二进制相位序列P_b。

4.根据权利要求3所述的基于信道特性的光OFDM动态密钥生成方法，其特征在于：所述步骤三中假设所要生成的密钥长度为M，需要量化的相位个数为N，则Q满足公式：$Q = 2^{\lceil \frac{M}{N} \rceil}$，其中$\lceil . \rceil$表示向上取整；量化后的$P_a$和$P_b$截取前M个值。

一种基于信道特性的光OFDM动态密钥生成方法

技术领域

[0001] 本发明提供一种基于信道特性的光OFDM动态密钥生成方法，为光OFDM物理层加密提供了动态密钥生成方案。

背景技术

[0002] 随着IPTV、高清电视、大型互动网络游戏等高速数据业务的发展，接入网的带宽需求将急剧增加。近年来，正交频分复用(OFDM)调制以其抗色散能力强、频谱利用率高等优点被引入光纤通信中。同时，它可以通过数字信号处理(DSP)方便地处理。此外，直接检测光OFDM系统(DD-OOFDM)具有结构简单、动态带宽分配灵活、异构服务透明、与现有网络兼容性好等优点而在下一代光接入网表现出巨大潜力。由于光接入网的物理层容易受到各种攻击，随着用户和网络容量的急剧增加，物理层安全问题变得越来越重要。以往的方法使用加密协议对数据帧进行加密，将安全问题放在网络的较高层次，因此在不安全的物理层基础上构建安全方案是有风险的。

[0003] 对现有文献的调查发现，现阶段的光OFDM物理层加密方案大都使用混沌序列对OFDM符号块进行频域和时域上的置乱。文献1[Zhang L,Xin X,Liu B,et al.Physical-enhanced secure strategy in an OFDM-PON[J].Optics Express,2012,20(3):2255-2265]提出了使用一维逻辑混沌映射生成n阶置乱矩阵P来加密频域OFDM信号，由于窃听者不知道混沌序列的初值、逻辑映射和迭代的步长，所以基本上很难恢复原始信号。文献2[Sultan A,Yang X,Hajomer A A E,et al.Dynamic QAM Mapping for Physical-Layer Security Using Digital Chaos[J].IEEE Access,2018,6:47199-47205]提出了四维逻辑映射方案，将每一个子载波上的符号幅度和相位进行了置乱，使其随机分布在一个圆形星座图内，其密钥空间巨大，加密效果显著。尽管对于光OFDM物理层加密研究成果较多，但现阶段的加密方案都是需要通信双方预先交换密钥初值，且一旦确定之后初值就不再改变，整个密钥都是静态的，这就降低了系统的安全性能。

发明内容

[0004] 本发明针对现有技术存在的不足，提供一种基于信道特性的光OFDM动态密钥生成方法，密钥随信道特性和随机探测信号实时变动，有效提升光OFDM系统的安全性。

[0005] 为达到上述目的，本发明是通过以下技术方案实现的：

[0006] 一种基于信道特性的光OFDM动态密钥生成方法，其中所生成的密钥是本地随机信号、接收到的探测信号与量化后的信道相位的异或结果，包括步骤如下：

[0007] 步骤一、发送端A生成随机二进制序列X_t并发送给接收端B；相干时间内，B生成随机二进制序列X_r发送给A；

[0008] 步骤二、发送端A估计携带信号X_r的N个子载波的信道特性，得到通信双方的信道响应：$|H_a^1|e^{j\theta_a^1}$，$|H_a^2|e^{j\theta_a^2}$，…，$|H_a^i|e^{j\theta_a^i}$，…，$|H_a^N|e^{j\theta_a^N}$，其中$|H_a^i|e^{j\theta_a^i}$表示发送端A第i个子载波的信道响应；接收端B估计携带信号X_t的N个子载波的信道特性，得到通信双方的信

道响应：$|H_b^1|e^{j\theta_b^1}$，$|H_b^2|e^{j\theta_b^2}$，…，$|H_b^i|e^{j\theta_b^i}$，…，$|H_b^N|e^{j\theta_b^N}$，其中$|H_b^i|e^{j\theta_b^i}$表示接收端B第i个子载波的信道响应；

[0009] 步骤三、将发送端A所有的θ_a^i进行量化得到二进制相位序列P_a；同理，接收端B将所有的θ_b^i量化后得到二进制相位序列P_b；

[0010] 步骤四、发送端A将得到的相位量化序列P_a与随机二进制序列X_r以及本地生成的二进制序列X_t进行异或运算生成密钥K_a；同理，接收端B将得到的相位量化序列P_b与随机二进制序列X_t以及本地生成的二进制序列X_r进行异或运算生成密钥K_b。

[0011] 所述步骤一中随机二进制序列以一定的调制方式加载到一个OFDM的数据子载波上作为随机探测信号，其中随机序列长度同密钥位数一致。

[0012] 所述步骤三中是将相位区间(0,2π]均分成Q个子区间，θ_a^i或θ_b^i落到相应的子区间内并进行对应的二进制编码，将发送端A所有的θ_a^i编码完成后按顺序合并为一个二进制相位序列P_a；将接收端B所有的θ_b^i编码完成后按顺序合并为一个二进制相位序列P_b。假设所要生成的密钥长度为M，需要量化的相位个数为N，则Q满足公式：$Q = 2^{\lceil \frac{M}{N} \rceil}$，其中$\lceil . \rceil$表示向上取整；量化后的$P_a$和$P_b$截取前M个值。

[0013] 本发明与现有技术相比具有如下优点：

[0014] 本发明提出的基于信道特性的光OFDM动态密钥生成方法，所生成的密钥不再是静态密钥，不需要通信双方约定好密钥初值，有效的提高了物理层安全通信的能力。本发明提出的动态密钥可以自动不定时的进行更新，产生的密钥结合其他加密技术，使得窃听者正确解密通信内容难度进一步加大，保密性能较现有技术进一步提升。本发明所生成的动态密钥只与通信双方间的信道特性和随机信号有关，通信双方在本技术方案下生成的最终密钥是一致的，获得的密钥可以用来更新混沌系统的初始值和参数以及作为其他数据加密算法的密钥。本发明适用于光OFDM系统，也适用于其他光通信加密系统的动态密钥生成。

附图说明

[0015] 图1为本发明光OFDM动态密钥生成过程示意图。

具体实施方式

[0016] 下面将结合附图对本发明的实施例做详细说明：本实施例在本发明技术方案为前提下进行实施，给出了详细的实施方案和操作过程，但本发明的保护范围不限于下述的实施例。

[0017] 本实施例是在光OFDM系统中进行，通信双方各自生成128位密钥序列，调制格式采用16QAM方式，子载波个数为64，有效数据子载波个数为28，整个动态密钥生成过程如图1所示，具体过程如下：

[0018] 步骤一、发送端A生成随机二进制序列X_t并发送给接收端B。相干时间内，B生成随机二进制序列X_r发送给A。

[0019] 步骤一所述的二进制序列X_t、X_r是和所需密钥长度一致的128位的随机二进制序

列，为了防止接收端译码过程中出现差错，上述的128位随机二进制序列可以采用一些纠错编码技术进行校验和纠错，最简单的比如奇偶校验。X_t、X_r经串并转换和16QAM调制后分别加载到各自的子载波上。

[0020] 步骤二、发送端A估计携带信号X_r的N个子载波的信道特性，得到通信双方的信道响应（$|H_a^1|e^{j\theta_a^1}$，$|H_a^2|e^{j\theta_a^2}$，…，$|H_a^i|e^{j\theta_a^i}$，…，$|H_a^N|e^{j\theta_a^N}$，其中$|H_a^i|e^{j\theta_a^i}$表示发送端第i个子载波的信道响应）；接收端B估计携带信号X_t的N个子载波的信道特性，得到通信双方的信道响应（$|H_b^1|e^{j\theta_b^1}$，$|H_b^2|e^{j\theta_b^2}$，…，$|H_b^i|e^{j\theta_b^i}$，…，$|H_b^N|e^{j\theta_b^N}$，其中$|H_b^i|e^{j\theta_b^i}$表示接收端第i个子载波的信道响应）。

[0021] 步骤三、将发送端A所有的θ_a^i进行量化得到二进制相位序列P_a；同理，接收端B将所有的θ_b^i量化后得到二进制相位序列P_b。其中，将相位区间(0,2π]均分成Q个子区间，$\theta_a^i(\theta_b^i)$落到相应的子区间内并进行对应的二进制编码，将发送端A(接收端B)所有的$\theta_a^i(\theta_b^i)$编码完成后按顺序合并为一个二进制相位序列P_a(P_b)。

[0022] 所述的Q满足公式：$Q = 2^{\lfloor \frac{M}{N} \rfloor}$，其中M是整个密钥长度(M＝128)，N为需要量化的相位个数(由于采用的是16QAM调制，可知需要的有效数据子载波个数N＝32)，计算得到Q值为16，即将(0,2π]均分成16个子区间((0,π/8]，(π/8,π/4]，…，(15π/8,2π])对应每个区间的相位量化二进制序列为(0000,0001,..,1111)。

[0023] 步骤四、发送端A将得到的相位量化序列P_a与随机二进制序列X_r以及本地生成的二进制序列X_t进行异或运算生成密钥K_a。同理，接收端B将得到的相位量化序列P_b与随机二进制序列X_t以及本地生成的二进制序列X_r进行异或运算生成密钥K_b。

[0024] $K_a=X_t \oplus X_r \oplus P_a$；

[0025] $K_b=X_r \oplus X_t \oplus P_b$。

[0026] 得到的合法通信双方的密钥序列是一致的，并且所获的密钥不仅与通信双方的信道特性有关，而且也与生成的随机二进制序列有关。该方法的动态密钥特性体现在信道特性会随着时间的改变而发生变化，并且用于探测信号的随机序列也是动态生成的。

[0027] 所生成的合法密钥只与收发两端的信道和随机信号有关，而窃听者不能获得与合法通信双方一样的通信信道以及不能攻击收发端设备获取合法收发端的随机二进制序列，所以攻击者几乎不能获得正确的生成密钥，并且合法密钥可以不定时的改变，该加密方案是很安全且有效的。所生成的合法密钥K_a和K_b可以用来更新混沌系统的初始值和参数以及作为其他数据加密算法的密钥。

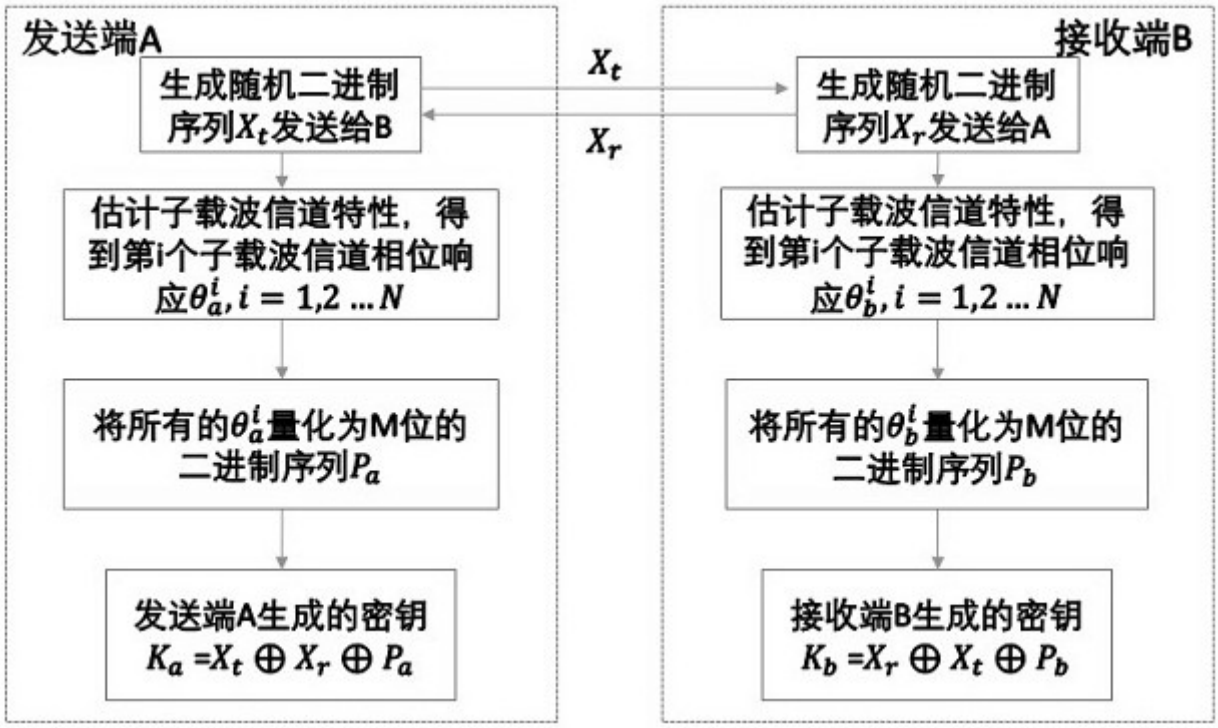

发送端A
生成随机二进制序列X_t发送给B
估计子载波信道特性，得到第i个子载波信道相位响应$\theta_a^i, i = 1,2 \ldots N$
将所有的θ_a^i量化为M位的二进制序列P_a
发送端A生成的密钥$K_a = X_t \oplus X_r \oplus P_a$
X_t
X_r
接收端B
生成随机二进制序列X_r发送给A
估计子载波信道特性，得到第i个子载波信道相位响应$\theta_b^i, i = 1,2 \ldots N$
将所有的θ_b^i量化为M位的二进制序列P_b
接收端B生成的密钥$K_b = X_r \oplus X_t \oplus P_b$

图 1